



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,904	12/01/2000	Bjorn Markus Jakobsson	38-2	3689

7590 11/24/2003

Joseph B. Ryan  
Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560

EXAMINER

BAYAT, BRADLEY B

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 11/24/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/727,904

Applicant(s)

JAKOBSSON ET AL.

Examiner

Bradley Bayat

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 04 September 2003.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

## Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_. 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

Claims 1-20 remain pending and are again presented for examination on the merits.

#### ***Response to Arguments***

Applicant's arguments filed September 4, 2003 have been fully considered but they are not persuasive.

Applicant asserts that the cited references (Nishioka and Kyojima) fail to teach or suggest all the claim limitations and there is no motivation for modifying the reference teachings to reach the claimed invention (response p.2). Applicant further contends that after reviewing the entirety of the Kyojima, applicant was unable to find "any mention of a signed ciphertext, much less a blinded version of a first ciphertext portion of a signed ciphertext (response pg. 3)." The applicant relies on the arguments set forth for claim one above, because the remaining claims are either dependent on claim one or include at least one such element.

In response to applicant's argument that the examiner has "failed to identify a cogent motivation" and relies on subjective conclusory statements, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Since the applicant's arguments rely on steps (a) and (b) of claim 1, the examiner provides the following steps below for purposes of discussion:

Art Unit: 3621

(a) receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

(b) decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

The examiner asserts that Nishioka discloses how entities on a communication network can utilize cipher communication methods in an electronic shopping system wherein a user desires to purchase products, however, the user does not desire the contents of the products purchased to become known to at least one of those entities (see columns 1-2). Nishioka explicitly discloses the need and desire on the part of the user to conduct electronic commerce without having to disclose the content of the purchase (column 2, lines 24-31). Nishioka further teaches how the legality of the digital signature  $\text{sgnA(P)}$  is confirmed, thereby authenticating the written order  $P=(P1, P2)$  utilizing predetermined ciphertext portions (columns 6-7; figures 11, 12 and associated text). Nishioka teaches how the proper entity is “notified of only the predetermined information, [accordingly, the] privacy of the user is protected (column 7, lines 42-62).”

Furthermore, Kyojima recognized security flaws in the prior art and thus applied a blind decryption method to securely transmit a specific piece of information to a decryption device while keeping the blindness of data delegated to be decrypted or to control access to such data (see background of the invention columns 1-4). Kyojima teaches how a decryption device decrypts a cipher text encrypted by RSA method (example of a digital signature), similar to claim 1 (see column 5-6). Kyojima further discloses that a user of the blind decryption device

Art Unit: 3621

possesses the cipher text C, a modulus n, the encryption key E (e.g., a digital signature) and the second decryption information d2 (see column 8). Kyojima further teaches that challenging plain data or its decryption result can be concealed from the proving device itself (columns 13-14).

Therefore, in the view of the teachings, the examiner asserts that it would have been obvious to one of ordinary skill in the art to modify Nishioka and utilize the teachings of Kyojima with respect to blind decryption to further secure and prevent an entity from accessing data that is not authorized to access.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishioka et al. (U.S. Patent 5,754,656) in view of Kyojima et al. (U.S. Patent 6,275,936 B1).**

As per claims 1-4 and 7-15, Nishioka discloses an electronic authenticating shopping method and system wherein selective information relating to a purchase request by a user is only known to a merchant and certain authentication information is obtained by a payment center (see column 2, lines 33-67; columns 3-7 and accompanying figures). Nishioka does not explicitly teach the use of a blinded ciphertext technique. Kyojima teaches a method to control access to digital data by applying a blind effect to a ciphertext and the use of a blind decryption method and access right authentication (see column 4, lines 57-67; columns 5-6 and 7-14 and

Art Unit: 3621

accompanying figures). Kyojima is evidence that one of ordinary skill in the art would recognize the benefit of utilizing a blind ciphertext decryption method to accomplish access control and authentication to digital data without disclosing unnecessary purchase information. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to utilize such techniques to accomplish the above stated purpose, as per teachings of Kyojima.

**Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishioka and Kyojima as applied to claim 1 above, and further in view of Zheng, U.S. Patent 6,396,928 B1.**

As per claims 5 and 6, Nishioka and Kyojima do not explicitly teach the use of an ElGamal encryption technique or the Schnorr signature scheme. Zheng teaches a method and system for performing digital message encryption and signature coding for use in communications and digital information systems, including ElGamal and Schnorr signature and encryption schemes or any suitable encryption algorithm, such as DES or the like (see column 2, lines 14-23; column 4, line 40 – column 5, line 67). Zheng is evidence that one of ordinary skill in the art would recognize the benefit of utilizing such techniques for secure authentication communication. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to utilize such techniques to accomplish the above stated purpose, as per teachings of Zheng.

Claims 16-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nishioka et al. (U.S. Patent 5,754,656) in view of Kyojima et al. (U.S. Patent 6,275,936 B1).

Art Unit: 3621

As per claims 16-20, Nishioka discloses an electronic authenticating shopping method and system wherein selective information relating to a purchase request by a user is only known to a merchant and certain authentication information is obtained by a payment center (see column 2, lines 33-67; columns 3-7 and accompanying figures). Nishioka does not explicitly teach the use of a blinded ciphertext technique. Kyojima teaches a method to control access to digital data by applying a blind effect to a ciphertext and the use of a blind decryption method and access right authentication (see column 4, lines 57-67; columns 5-6 and 7-14 and accompanying figures). Kyojima is evidence that one of ordinary skill in the art would recognize the benefit of utilizing a blind ciphertext decryption method to accomplish access control and authentication to digital data without disclosing unnecessary purchase information. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to utilize such techniques to accomplish the above stated purpose, as per teachings of Kyojima.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

Art Unit: 3621

calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Z. A. Ramzan, "Group Blind Digital Signatures: Theory and Applications," MIT, May 1999.
- Patent No. 5,715,314 to Payne et al., Network Sales System.

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley Bayat whose telephone number is 703-305-8548. The examiner can normally be reached on Tuesday-Friday during normal business hours.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 703-305-9768. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-306-5484.



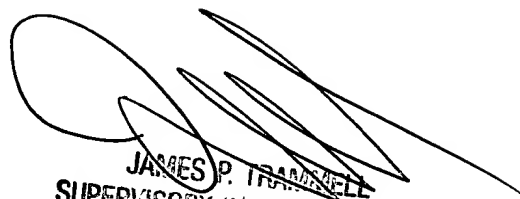
Application/Control Number: 09/727,904

Page 8

• Art Unit: 3621

bbb

November 13, 2003



JAMES P. TRAMMELL  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600